EXHIBIT C

May 10, 2017

The Honorable Brian Kemp
214 State Capitol
Atlanta, Georgia 30334
(Via email tfleming@sos.ga.gov)

Dear Secretary Kemp:

We write to request your prompt review of Georgia's voting system under the provisions of Georgia Code §21-2-379.2 to assess whether the current voting system "can be safely and accurately used" in the June 20 Congressional District 6 election. Georgia has a long history of voter concerns related to the unverifiable touchscreen voting system with no paper trail. Concerns have escalated because of recent unresolved security issues, as well as the heightened risk of cyber attacks in the current environment. We respectfully request that your office undertake, at a minimum, a partial review of the system to determine whether specific hardware, software, and procedures can be safely and accurately used as required by §21-2-379.2, and separately whether the system is in compliance with applicable federal and state election standards.

Given the indisputable escalation of cyber-security threats in the 15 years since the Diebold system was deployed, this examination is essential for public confidence and security of the upcoming June 20 election. Given the unprecedented national interest in the runoff election, we urge your office to undertake this work immediately. In the likely event that system security deficiences are detected, officials should implement a paper ballot election.

To define the highest-priority areas for our requested review, we have conferred with computer scientists experts in voting system security. We are not seeking a complete "top-to-bottom" certification and laboratory system testing review prior to the conduct of the June 20 election. We are not requesting an immediate recertification of the system. Instead, we request that you initially respond to our concerns by reference to system records. Responses to our listed concerns should be readily available in your office's existing records, staff knowledge and resources, and through conferral with the Center for Election Systems at Kennesaw State University.

We are Georgia electors who believe that the national attention focused on the June 20 special election calls for increased scrutiny concerning the transparency, security, and verifiability of our voting system.

We believe that responses to our listed concerns can be answered within a few hours by knowledgeable staff of your office and the Center for Election Systems. The cost of this reexamination should be modest, and should be borne by the state, not by private citizens. We respectfuly request that you charge only de minimis amounts or waive the requirement that requesting citizens bear the cost of this essential examination conducted for the benefit of all Georgia voters.

The priority areas related to ***safety and accuracy*** of the system listed below must be satisfactorialy addressed in a publicly available report prior to the June 20 election.

Priority areas related to ***safety and accuracy*** of the system include:

1. March 15 Computer Scientist Inquiry
   Leading voting system computer scientists expressed their concerns about Georgia's system and urged you to move the state forward to a system of paper ballots in their March 15 letter attached as Exhibit A. It is our understanding that no response was received from your office. Please address the concerns raised in the letter by disclosing the conclusions made by your office and any mitigating actions taken or planned.

2. Database design
   The attached research, *GEMS Tabulation Database Design Issues in Relation to Voting Systems Certification Standards* by Thomas P. Ryan and Candice Hoke (Exhibit B), presents architecture flaws in the GEMS database design that create unacceptable risks of inaccurate tabulation and reporting. What mitigation has been employed to address these vulnerabilities, and how have any mitigation efforts been tested for adequacy?

3. Malicious attack code threat
   The attached research, *Security Analysis of the Diebold AccuVote-TS Voting Machine* by Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten (Exhibit C), presents detailed and important security weaknesses in the Diebold system. Section 2.2 explains various ways that attack code could be installed. The referenced work is also summarized in these two video recordings—one from a Congressional hearing (https://www.youtube.com/watch?v=HBqGzgxcfAk) and one in a laboratory setting (https://www.youtube.com/watch?v=aZws98jw67g). Have the security weaknesses presented in these videos been mitigated to ensure that the machines can be used "safely and accurately" without realistic security attacks? If so, please provide a description and date of the mitigation efforts.

4. Security of electronic transmission of votes and results
   Votes and results are transmitted via modem from PCMCIA TS memory cards to GEMS servers. Are these election night transmissions of memory card data secured through cryptographic means to prevent interception and possible alteration on their way to the GEMS servers? If so, please provide a description and effective date.

5. Memory card security
   What system software protections prevent the introduction of substituted or modified TS PCMCIA cards prior to TSx uploading to the GEMS server? What system controls are in place to ensure that all precinct cards have been collected and successfully uploaded? What measures prevent forged or maliciously programmed voter access or supervisor cards from transmitting malware to the voting machines?

6. Accessibility of audit logs
   In compliance with VVSG2002 2.2.4.2 and 2.2.5, are cast vote records, TS and TSx audit logs, OS audit logs, and GEMS audit logs readily exportable in human-readable format reports to permit officials, observers, and members of the public to timely review and verify against reported totals? Do current procedures require review of such audit logs for signs of irregularities or system errors?

7. Internet exposure
   What specific guidelines and required processes prevent connecting TS or TSx voting machines or the GEMS servers to the Internet either directly or through the use of removable media (such as flash memory cards) that have been exposed or connected to the Internet?

8. Uploading protocols
   What specific guidelines, required processes, and/or software mechanisms are in place to prevent improper election data, including cast votes, from being uploaded to the GEMS servers either because of human error or software or hardware failures?

9. Encryption key disclosure
   Was the system upgraded and secured against malicious use of the encryption key after it was erroneously published on the Internet? If so, please disclose the date and version numbers of software upgrades or repairs that address the system security issues presented by the widespread knowledge of the system encryption key.

10. ExpressPollbook software flaws
    At the April 22 meeting, the Fulton County Election Board discussed pollbook software errors that caused voters to be sent to improper precincts during the April 18 election. Please explain the source of the software problems and what mitigation steps have been taken to protect the June 20 election from this software issue's harmful impacts and potential voter disenfranchisement.

11. Physical security of voting machines (DREs)
    How are DREs protected from intrusion when not in use, including storage before and after they are delivered to the polling place and during warehouse storage after the election? Given the large number of machines, polling locations, and ease of concealing physical intrusion into the machines, we are concerned that is it impractical to ensure that machines are protected from intrusions that can implant malware. Please reference Exhibit C, section 2.2.1.

12. Compliance with certification standards
    Is the system as currently configured and used certified under federal standards? What standards of certification are required for this specific system configuration under current Georgia law? Is the state certification documentation current?

We are concerned that the system cannot be used safely and accurately, particularly if deficiencies are identified in any of the above controls. As noted in the *Security Analysis of the Diebold AccuVote-TS Voting Machine*, Section 5.4 in Exhibit C, even if the current system configuration is certified to VVSG2002 standards, such certification ***does not imply that the system can be "safely and accurately used"*** as §21-2-379.2(c) requires.

The above list of priority areas is not comprehensive. As we continue to confer with voting system computer scientists, we may amend this letter to add other urgent concerns or remove any less urgent concerns.

We do not seek any proprietary information or security details that would compromise the security of the voting system. Instead, we request a description of the type of review undertaken and a general description of any mitigation adopted that would assure the public that the system is free from previously disclosed security risks.

The software versions we understand to be in current use are listed on Exhibit D. Please inform us if our understanding is inaccurate, and please supply a list of currently installed software.

We also request a copy of the most recent certification documentation for the current voting system and its compliance with applicable Georgia law and election rules.

Dr. Duncan Buell is our technical adviser and contact point for purposes of discussions with your office. You may contact him through buell@acm.org and 803-479-7128. Dr. Buell is the NCR Chair in Computer Science and Engineering at the University of South Carolina and a voting systems expert.

Thank you for your prompt consideration of our request.

Sincerely,

Mustaque Ahamad
Atlanta, GA 30306

David Bader
Atlanta, GA 30306

Ricardo Davis
Woodstock, Georgia 30188

Richard DeMillo
Atlanta GA 30305

Virginia Forney
Atlanta, GA 30309

Merrick Furst
Atlanta 30306

Adam Ghetti
Atlanta, GA 30324

Jeff Levy
Atlanta, GA 30306

Rhonda J. Martin
Atlanta, GA 30305

Paul Nally
Rydal, GA 30171

Michael S Optiz
Marietta, GA

cc: DeKalb County Elections, H. Maxine Daniels, Director voterreg@dekalbcountyga.gov
Fulton County Elections, Director Richard Barron Richard.Barron@fultoncountyga.gov
Cobb County Election Director Janine Eveler, info@cobbelections.org